学校编码：10384　　分类号_____密级_____
学号： X2011231102　　UDC _____

厦门大学

工 程 硕 士 学 位 论 文

基于蜜网的攻击目标构建方法研究

Research on Attack Target Construction Based on Honeynet

程 曦

指 导 教 师： 董 槐 林 教 授
专 业 名 称： 软 件 工 程
论文提交日期： 2013 年 10 月
论文答辩日期： 2013 年 11 月
学位授予日期： 年 月

指 导 教 师：_____
答辩委员会主席：_____

2013 年 10 月

厦门大学学位论文原创性声明

本人呈交的学位论文是本人在导师指导下,独立完成的研究成果。本人在论文写作中参考其他个人或集体已经发表的研究成果,均在文中以适当方式明确标明，并符合法律规范和《厦门大学研究生学术活动规范（试行）》。

另外，该学位论文为（　　）课题（组）的研究成果，获得（　　）课题（组）经费或实验室的资助，在（　　）实验室完成。（请在以上括号内填写课题或课题组负责人或实验室名称，未有此项声明内容的，可以不作特别声明。）

声明人（签名）：

2013 年　月　日

厦门大学学位论文著作权使用声明

本人同意厦门大学根据《中华人民共和国学位条例暂行实施办法》等规定保留和使用此学位论文，并向主管部门或其指定机构送交学位论文（包括纸质版和电子版），允许学位论文进入厦门大学图书馆及其数据库被查阅、借阅。本人同意厦门大学将学位论文加入全国博士、硕士学位论文共建单位数据库进行检索，将学位论文的标题和摘要汇编出版，采用影印、缩印或者其它方式合理复制学位论文。

本学位论文属于：

（　　）1.经厦门大学保密委员会审查核定的保密学位论文，于　　年　　月　　日解密，解密后适用上述授权。

（　　）2.不保密，适用上述授权。

（请在以上相应括号内打“√”或填上相应内容。保密学位论文应是已经厦门大学保密委员会审定过的学位论文，未经厦门大学保密委员会审定的学位论文均为公开学位论文。此声明栏不填写的，默认为公开学位论文，均适用上述授权。）

声明人（签名）：

2013 年　月　日

摘 要

网络攻击训练平台为提高我国广大网民的信息安全意识和网络防护技术提供了重要支撑，而攻击目标作为网络攻击训练平台的重要组成部分，其构建的好坏则直接影响整个训练平台的最终效果。与此同时，蜜网技术作为一种新型的主动防御网络安全技术，已经受到信息安全领域的重视[1, 12,20]。

本文利用蜜网系统构建网络攻击目标。首先，深入研究分析了虚拟蜜网技术，介绍了蜜罐、蜜网、真实蜜网、虚拟蜜网的概念，重点阐述了虚拟蜜网的实现方法及蜜网网关 Roo；其次，归纳了现有的网络攻击方法和攻击目标构建方法，设计了系统级和应用级的攻击目标构建方案，并对攻击目标配置方法进行了研究；然后，基于 VMware 构建了虚拟蜜网系统，给出了虚拟蜜网的拓扑结构和网络配置，重点介绍了 VMware workstation 和 Honeywall Roo 的安装与配置；最后，设计并实现了基于蜜网系统的攻击目标构建，阐述了网络攻击训练的原理和流程，搭建了攻击目标测试环境，配置了网络攻击目标，并利用网络攻击训练平台对攻击目标进行攻击测试。

本文利用网络攻击训练平台了解黑客的攻击目的、攻击方法和攻击工具，为提高信息安全防范能力提供了技术支撑。

关键词：蜜网；网络攻击目标；攻击测试

Abstract

Network attack training platform provides an important support for enhancing information security awareness and security protection technology of the internet users, attacking targets is an important part of it, its success directly affects the ultimate effect of the whole training platform. In the meantime, honeynet technology, as a new type of the active defense network security technology, has been valued by information security.

This dissertation establishes network attack targets by honeynet system. Firstly, we do some in-depth researches and analysis of virtual honeynet technology, introduce the concepts such as honeyhot, honeynet, real honeynet, virtual honeynet, and focus on explaining the implement methods of virtual honeynet and honeynet gateway Roo; secondly, we conclude current methods of network attack and establishing attack targests, design system-level and application-level construction plan of establishing attack targets, and research the configuration method of attack targets; afterwards, we establishes the virtual honeynet system based on VMware and give the topological structure and network configuration of virtual honeynet, focus on introducing the installment and configuration of VMware workstation and honeywall Roo; finally, we design and realize the establishment of attack targets based on honeynet system, explain the theory and process of network attack training, set up testing environment of attack targets, complete the configuration of network attack targets and make an attack test of targets by network attack training platform.

This dissertation provides an important support for understanding the purposes, methods and tools of hacker attack, enhancing the prevention capacity of information security.

Key Words: Honeynet; Network Attack Target; Attack Test

目 录

Contents

第一章 绪论

1.1 研究背景和意义

根据国家计算机网络应急技术处理协调中心 CNCERT/CC 的《2012 中国互联网网络安全报告》统计，2012 年 CNCERT 抽样监测结果显示，在利用木马或僵尸程序控制服务器对主机进行控制的事件中，控制服务器 IP 总数为 300407 个，较 2011 年下降 39.1%，受控主机 IP 总数为 27275399 个，较 2011 年大幅增长 71.1%；全球互联网平均每月有超过 3500 万个主机 IP 感染“飞客”蠕虫，排名前三的国家或地区分别是美国（16.1%）、中国大陆（11.6%）和巴西（7.4%），境内感染“飞客”蠕虫的主机 IP 月均超过 400 万个；恶意程序传播事件 35821698 次，其中恶意程序下载链接 785388 个，“放马站点”域名 67468 个，“放马站点”IP 地址 55673 个；CNCERT 共接收国内外报告网络安全事件 15366 起，较 2011 年增加了 47.3%。同时，应用软件漏洞数量急剧增加，国家信息安全漏洞共享平台在 2011 年发布了 5547 个漏洞，较 2010 年增加了 60.9%，其中，高危漏洞 2164 个；网站用户信息安全措施严重缺乏，特别是在 2011 年底，CSDN、天涯论坛等网站的大量用户信息遭到泄露，涉及账号、密码信息 2.87 亿条。由此可见，我国广大网民所处的网络安全环境正越来越恶劣。

工业和信息化部在 2012 年中国计算机网络安全年会上指出，随着网络的 IP 化、宽带化、智能化以及新技术新业务新业态的快速发展，网络安全问题更加复杂，形势依然严峻。随着“两化”融合的深入推进和全社会信息化水平的不断提高，通信网络的基础性和战略性地位更加突出，为我国的信息化建设和经济社会又好又快发展提供了基础保障和强大动力。但与此同时，网络攻击、信息窃取、病毒传播等安全事件和违法犯罪活动多发频发，社会各界和广大用户要求加强电信用户信息保护的呼声日益强烈，通信网络仍然存在一些安全隐患和薄弱环节，核心技术与关键资源的自主可控能力不强，网络安全方面的高精尖人才还比较缺乏，全社会网络安全意识仍有待进一步提高[1]。

为防止各种入侵事件的发生，提高系统的安全性，人们采取了多种安全防护手段，包括身份认证技术、访问控制技术、数据加密技术、反病毒技术、防火墙技术等[2]。然而这些传统的计算机安全防御手段发挥作用的前提是必须对现有系统的安全漏洞具有全面的了解和掌握，处于一种被动防御的局面，同时缺乏对入侵者的了解，即谁在攻击、

攻击的目的是什么、如何进行攻击等。因此，只有寻求一种主动的网络安全防御方法，才能使自己的计算机在网络上保持安全，才能对网络威胁做出相应的有效的安全防御措施。正是在这种情况下，蜜罐技术应运而生，为实现主动的网络安全防御提供了可能。蜜网系统是一种体现主动防御思想的安全资源,其价值在于被探测、攻击及被攻陷后记录入侵信息，蜜网系统本质是由若干具备收集和交换信息能力的节点构成的分布式诱捕系统蜜罐通过真实或模拟的网络和服务来吸引攻击，从而可以在入侵者攻击蜜罐期间对其行为和过程进行记录分析和研究，进而发现新型攻击，检索新型黑客工具，了解黑客和黑客团体的背景、目的、活动规律等。

同时，互联网的高普及率和网民数量的激增使得网络黑客攻击的范围更广、威胁更大，广大网民薄弱的网络安全意识也让网络黑客有机可乘。如何让广大网民能够直观全面的了解黑客的攻击行为、深入分析黑客的攻击手段，掌握网络安全防护知识甚至是网络攻击的原理和方法，并最终将网络安全专业知识应用于实际，提高网络安全防护能力成为了一个重点和难点问题。为此，人们设计并实现了网络攻击训练平台来达到这一目的。网络攻击训练平台包括攻击端、管理端、监控端和被攻端四个部分，其中被攻端的设计是网络攻击训练平台设计的一个关键环节，而攻击目标的构建则是被攻端需要完成的主要工作[2]。

本文正是从此目的出发，结合蜜网系统的优势构建攻击目标。基于蜜网技术构建的攻击目标为网络攻击训练平台提供了一个可在实际环境中进行真实网络攻击训练的实验环境，通过攻击实战，实现一些常见的网络攻击训练，从而使得用户掌握基本的网络安全知识，对网络做出更好的安全保护。

1.2 国内外研究现状

1．国外研究现状

1999 年，由 Lance Spitzner 等人成立蜜网技术邮件组，成立之初是一个非正式的组织，仅为了安全分析人员间进行蜜网技术的学习和交流。2000 年 6 月，蜜网技术邮件组发展成为正式的“蜜网项目组”(Honeynet Project)，开展对蜜网技术的验证和研究[3,13,22]。2002 年 1 月，为了联合与协调各个国家共同研究蜜网技术，对黑客团体进行追踪和学习，成立了“蜜网研究联盟”(Honeynet Research Alliance)。蜜网研究联盟的主要任务是通过使用蜜网技术来诱骗黑客，并分析攻击者的攻击技术、攻击动机和攻击工具，